International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 4, Aug 2014, 47-58

A NOVEL APPROACH FOR MULTIMEDIA ENCRYPTION BASED ON CONFUSION AND CHAOTIC LOGISTIC MAP

BRIJESH KUMAR PATEL & N. S. RAGHAVA

Department of Information Technology, Delhi Technological University, New Delhi, India

ABSTRACT

The process of exchange of information between two or more entities is known as data communication. It may evolve data in different format, such as text, images, audio and video, etc. Now- a- days, data in the form of images are used in a wide range of applications, like in medicine, in military operations and communication purposes. To safeguard multimedia information from imposters during transmission through communication channels, security measures are required, which can be achieved by the process of encryption. In this paper, we have proposed a multimedia encryption techniquecentered on confusion and diffusion of data at the pixel level. After encoding discrete cosine transform (DCT) is applied to further diminish the volume of multimedia information. The throughput of various experiments and sensitivity test proofs that proposed method works effectively for real time data encryption and security. An image shuffling method and chaotic logistic map are used for confusion and data encryption/decryption in the proposed method.

KEYWORDS: Chaotic System, Confusion and Diffusion, Discrete Cosine Transform (DCT), Logistic Map,Shuffling

INTRODUCTION

Now-a-days, multimedia encryption has found a lot of attention in the field of image processing and data communication. Multimedia deals with different forms of information such as text, images, audio and video. For any data encryption/decryption ciphering is the process in which data is represented in some other form to protect it against eavesdroppers, while deciphering is the process to recover or obtain original data from encoded information[4-6]. In the last decade, numerous chaos based multimedia encryption scheme has been devised. Chaotic maps have voluminous fundamental property such as unpredictability or randomness and mixing properties. These properties can be considered equivalent to some cryptographic topographies such as diffusion;confusion. Chaotic maps have been used in several different manners in multimedia security. The most important application of one-D and two-D chaotic maps is a pseudorandom number generator, which intern used to cipher block for data encryption [7-8].

In this paper, a newmethodology for multimedia encoding scheme is proposed based on bit shuffling and the chaotic logistic map in order to satisfy the real time protected data transmission. In this encoding technique first confusion is created by bit shuffling and after that a block of cipher having image size, i.e. M x N is applied to finally encryption of data, Where M and N represent rows and columns of image (Plain text) respectively. Pixel shuffling before encryption develops confusion, which enhances security of multimedia encryption before the block level image encryption[9-10].

PREVIOUS WORK

In the field of multimedia encoding using chaotic logistic maps a lot of work had been done in the past, which includes image encoding method on the basis of a chaotic logistic map produced by N.K. Pareek, Vinod Patidar, K.K. Sud[7],

partial image encoding, using a chaotic logistic map by NitumoniHazarika and Mon Jul Saikia. In the first one, they have generated two dimensional random numbers and uses bitwise XOR operation to generate an encoded image, whereas in the second approach they partially encrypted image and performed DCT transform to reduce data size[11].

These above two methods of digital data security, totally depends on the seed (encryption matrix) which is created based on the initial parameters of the chaotic maps. Once, if the initial parameters are known to intruders the security provided by these above mentioned methods can be compromised. Therefore, for making the system more efficient some new method requires to apply which will provide better security for all kinds of multimedia information [12-13].

PROPOSED METHOD

We propose an efficient algorithm for multimedia security, which provides better security than earlier chaotic based encryption systems. Multimedia encryption using our proposed method is a four-step process. In the first we create confusion by changing bit positions in the input image. In the next step a block of random numbers is created by applying iterations as many times as the image size. Then the XOR operation is applied to generate the cypher text (encrypted image). Finally, discrete cosine transform (DCT) is applied to shrink the volume of data by compression. In the decryption, we performed reversed of the encoding process at the receiver's end.

Chaotic Logistic Map

The word chaos means randomness in the system. It is the measurement of disorder into a system. In case of data encryption it can be considered as how much cipher block is sensitive to the initial conditions of the chaotic maps. Chaotic map, which we have applied in our proposed method of multimedia encryption, is mathematically represented by the formula given below

$$F(X_n) = aX_n(1-X_n) \quad (1)$$

$$F(X_{n+1}) = F(X_n) \quad (2)$$

Here X_n represents the chaotic sequence [3], which lies between zeroand one, as shown in Figure 2. The preliminary condition in case of the logistic map is for n=0, $X_0 \in [0, 1]$.

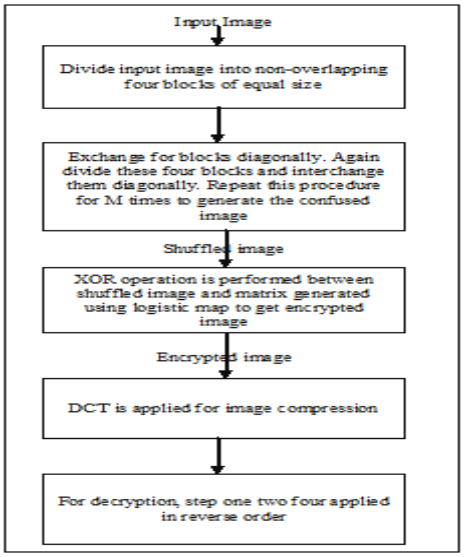

Figure 1: Flow Chart of Proposed Algorthim

The parameter 'a' is a real number in the range of 0 and 4, i.e. a ∈[0, 4]. After a lot of research, researchers have found that system is chaotic for 'an' in the range from 3.56994 < a ≤ 4. For the value of 'a' beyond 4, the value of X leaves ranges [0, 1]. And X_n diverges for almost all initial values of X_0. Depending on the values of 'a', X has different nature, which are shown in the Figure 2.

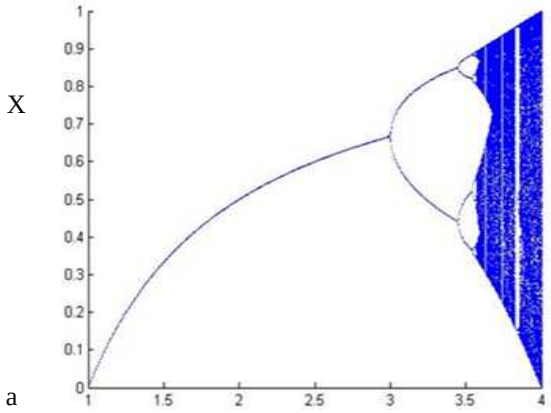

Figure 2: Bifurcation Diagram for Logistic Map

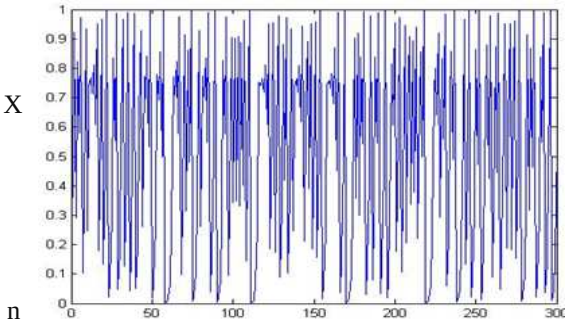

Figure 3: Variation of Chaotic Logistic Map with Iteration

We used the chaotic logistic map, in this encryption process, because even if we know the initial condition, we can't predict what will be the value of X_n at a given iteration n, since there is no direct relation between them. One of the major advantages of using chaotic system is its low cost in the signal generation process. Image encryption using chaotic systems divided into two broad categories, block cipher based encryption and stream cipher based encryption. In our proposed method we have used block cipher based technique for multimedia encryption.

PROPOSED ALGORITHM

Our proposed algorithm for multimedia encryption is a five-step process

- Divide the input image into four equal components.
- Image is shuffling to create confusion.
- Encryption of information using a logistic map.
- DCT is applied to the encrypted image for compression.
- Step 1-4 is applied in reverse order to get the original image.

Image Shuffling Process

Step 1

In the first iteration split the original image into four equal

Components and interchange them diagonally.

Figure 4:Input Image

Figure 5: Image after First Iteration

Step 2

Now, in the second, third, fourth and fifth iterations, again divide the each component of the shuffled image into four components and interchange them diagonally.

Step 3

Repeat step number one, for N (where N is an integer) iterations to generate shuffled image.

Figure 6:Shuffled Image after Fifth Iteration

Encryption Using a Chaotic Logistic Map

Shuffled image is encoded applying the pseudorandomsequence derived from the chaotic logistic map.

Step 1

Choose the initial value of the constant parameter 'a' and X_0 for chaotic logistic map. These parameters act as secret symmetric key for data encryption using logistic map.

Step 2

Logistic map work as a key stream generator for encoding.Thedimensions of the stream depend upon the dimensions of images taken in the encryption process. If the image size is M×N, then the number of logistic sequence will be 8×M×N obtained by equation (1).

Step 3

Encoding is done by bitwise Exclusive-OR operation between shuffled image and sequence generated in step 2.

Step 4

Discrete cosine transform (DCT) is applied to the encrypted image, for compression.

Step 5

At the receivers end, step 1-4 are applied in reverse manner to recover the original image.

EXPERIMENTAL OUTCOMES AND DISCUSSIONS

In this section, we have shown the experimental results of the proposed image encryption algorithm to appreciate the efficiency of the encoding technique. The MATLAB 7.5 software was used for executing this code. Here, we have taken a test image of size 256 x 256 is shown in figure 7(a). The initial parameters for logistic map are chosen as a=3. 999 and X_n = 0.1 to make the chaotic system. Secret symmetric key for encoding is a combination of X_0 = 0. 1 and a = 3. 999. Figure 7(b) is the shuffled image and figure 7(c) is encrypted image respectively.

ENCRYPTION PROCESS BY LOGISTIC MAP

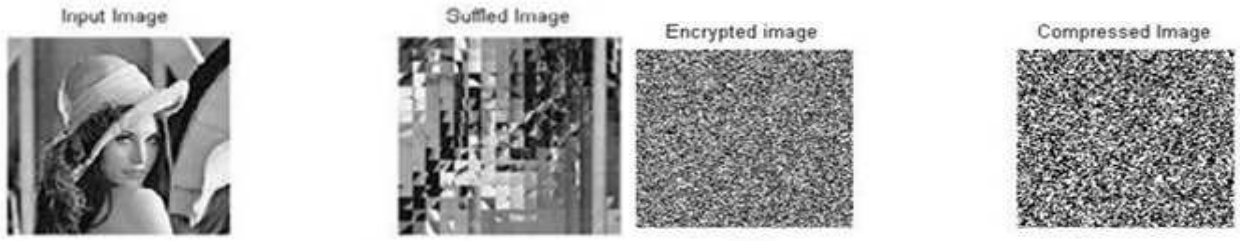

Figure 7(A), Figure 7(B),Figure7(C) and Figure 7(D): Represents the Input, Shuffled, Encrypted and Compressed Images Respectively

DECRYPTION PROCESS BY SUFFLING AND LOGISTIC MAP

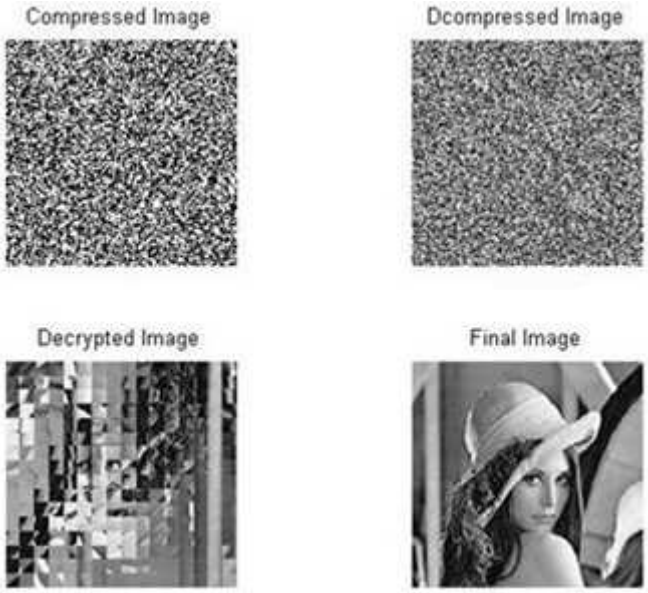

Figure 8(A), Figure 8(B), Figure 8(C) and Figure 8(D): Respectively Represents the Compressed, Decompressed, Shuffled and Final Images after Decoding

The proposed method for multimedia encryption works as well for color images also.

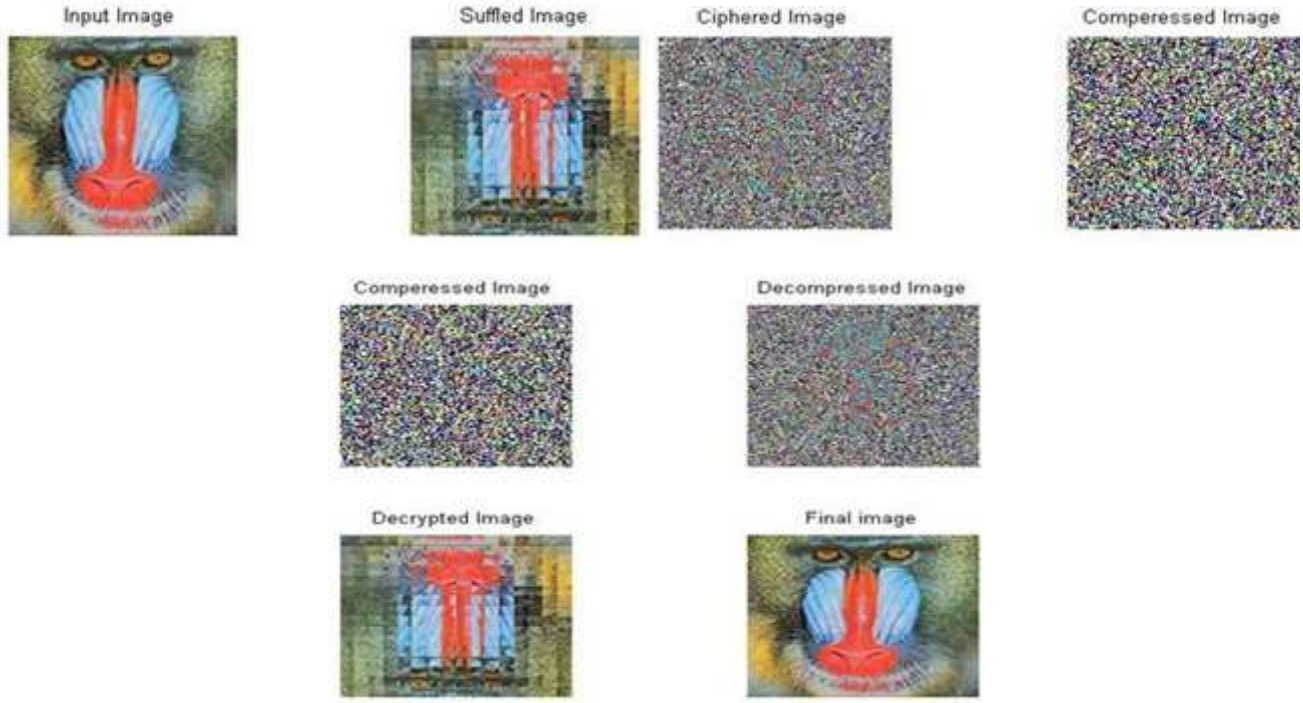

Figure 9(A), Figure 9(B), Figure 9(C) and Figure9(D): Represents the Input, Shuffled, Encrypted and Compressed Color Images Respectively. Whereas Figure10(A), Figure 10(B), Figure 10(C) and Figure 10(D): Respectively Represents the Compressed, Decompressed, Shuffled and Final Color Images after Decoding

HISTOGRAM ANALYSIS

The histogram of an image is the graphical representation of pixel intensities. In a given figure, it tells how the pixel value gets distributed. In case of gray image 256 different intensity values possible, so in the graphical representation histogram will display 256 intensities and the distribution of pixels among those intensities.

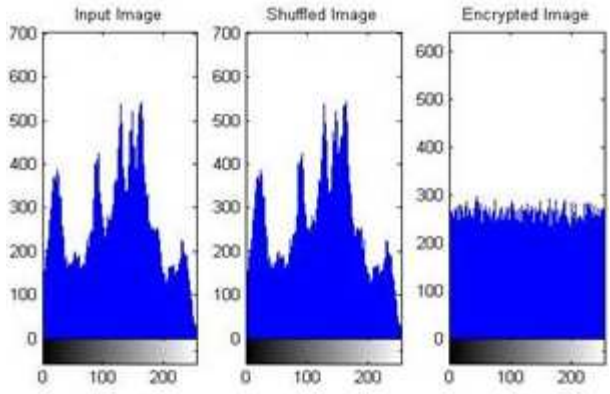

Figure 11(a) Figure11(b) Figure11(c)

Figure 11(A), Figure 11(B) and Figure 11(C): Are the Histograms of Original Images, Shuffled Image and Encrypted Image Respectively

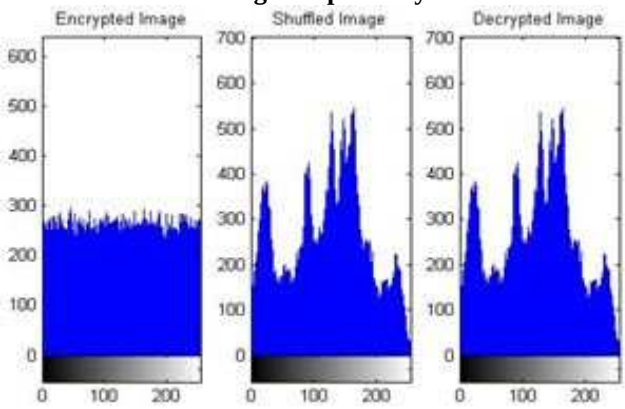

Figure 12(a)Figure 12(b)Figure 12(c)

Figure 12(A), Figure 12(B) and Figure 12(C): Represents the Histograms of Ciphered Image, Shuffled Image and Final Image Recovered Fromthe Shuffled Image Respectively

KEY SENSITIVITY TEST

For secure encoding, the key should be sensitive to large spaced key size to avoid everykind of conceivable attack. Randomness is the key point of the logistic map. To test the sensitivity of the key involved, a minute variation was done in original secret key by changing it from

X_0 from 0.1 to 0.10001. As a result, it is not possible to obtain the original image at the receiver's end.

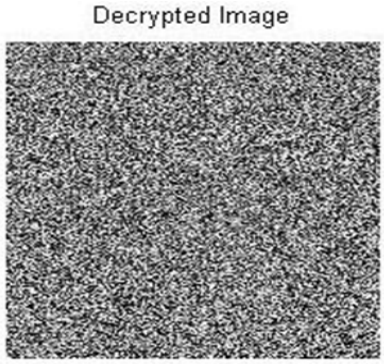

Figure13(a): Is the Decrypted Image after Slight Variation in Decryption Key

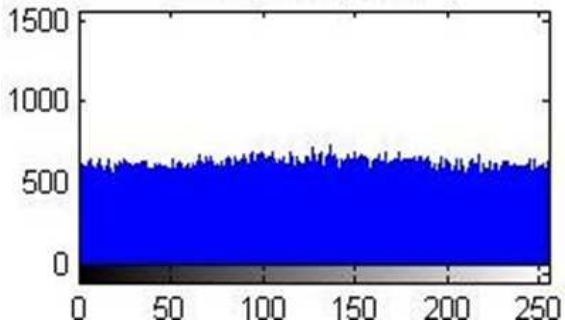

Figure 13(b): Is the Histogram of the Decrypted Image

INFORMATION ENTROPY ANALYSIS

Information entropy is the degree of uncertainties in the encryption scheme. It is used to evaluate the Effectiveness of image encryption algorithm. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.

Entropy is defined as

H = -sum (p.*log2 (p))(3)

The idyllic entropy of an encrypted image should be equivalent to 8, which corresponds to a random source. Practically, info entropy is less diverse than the ideal one. The values calculated in Table 1 are very close to the ideal value.

Table 1: Entropy Analysis

	Input Image	Encrypted Image	Decrypted Image
Entropy	7.8439	7.9990	7.8440

MEAN VALUE ANALYSIS

Mean value analysis is done to validate the distribution of mean pixel gray value in every vertical line of an image. It also gives the average intensity of pixels along the horizontal direction in the image. In a plain image, the mean value differs along the horizontal direction and has wide variations in the mean across the width of the image.

In an encrypted image the mean value along the horizontal direction should remain consistent, which indicates the uniform distribution of gray levels along all vertical lines of the encrypted image. Figure. 14 show the mean value obtained from the encrypted gray scale images by applying the proposed encryption method.

Here red line is for the original image and the green line is for encrypted image. The mean value across the image remains nearly consistent and close to each other.

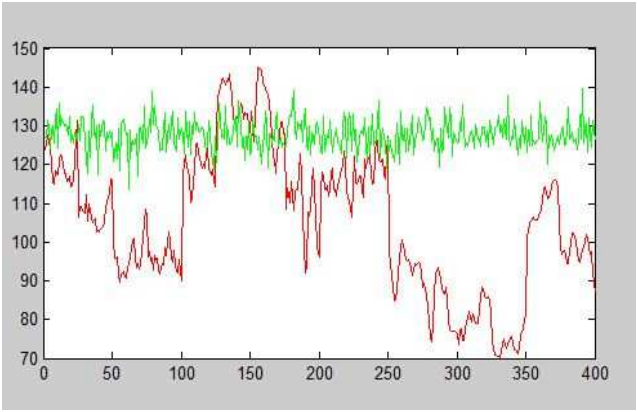

Figure 14:Mean Values of Original Image and Encrypted Image

ENCRYPTION KEY RANDOMNESS ANALYSIS

For better performance of the proposed algorithm, key values generated from chaotic maps should differ from neighboring keys to a larger extent. Here, from the Figure 15 it's clear that following property is satisfied by the key generated using a chaotic logistic map.

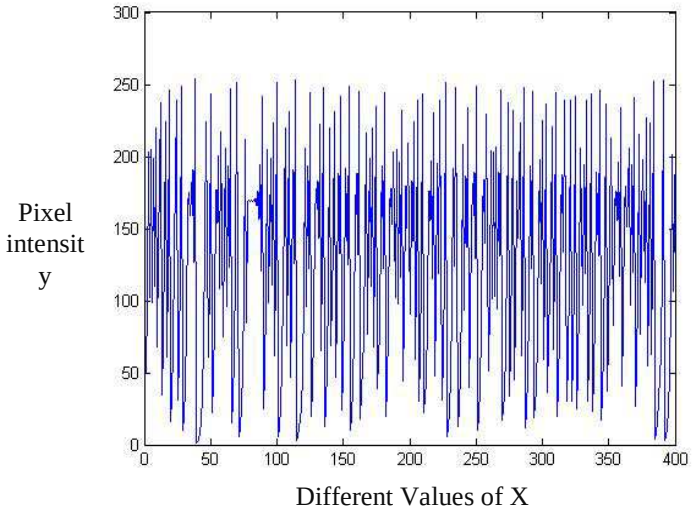

Figure 15: Encryption Key Randomness Analysis

RESULT COMPARISION WITH HENON MAP

Table 2: A. ENTROPY

	Logistic Map	Henon Map
Input image	7.8439	7.4521
Encrypted image	7.999	7.9406
Decrypted image	7.8440	7.4522

KEY SENSITIVITY COMPARISION

(a) Logistic map

Encryption key X_0changes from 0.01 to 0.010001.

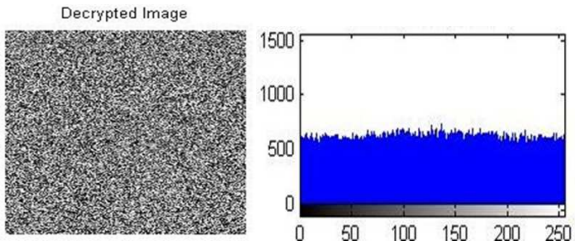

Figure 16(a) **Figure 16(b)**

Figure16(A): Is the Decrypted Image after Slight Variation in the Encryption Key for Logistic Map
Figure 16(B): Is the Histogram of Decrypted Image

HenonMap

Encryption key x1= 0.01 andy1= 0.02 changes to x1 = 0.010001 andy1= 0.020001.

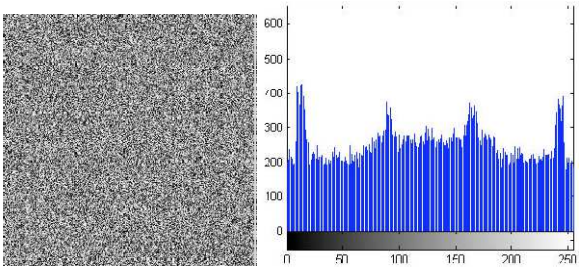

Figure 17(A)Figure 17(B)

Figure 17(A): Is the Decrypted Image after Slight Variation in the Encryption Key for Henon Map
Figure17(B): Is the Histogram of Decrypted Image

MEAN VALUE COMPARISION

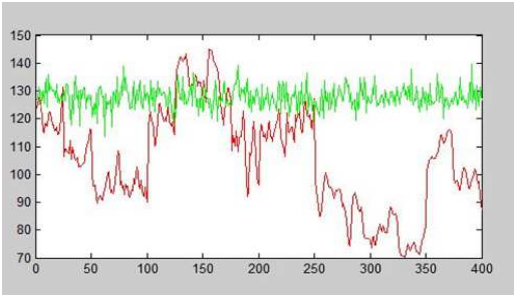

Figure 18(A)

Figure 18(A): Is the Mean Value Analysis of Original Image and Encrypted Image Using Logistic Map

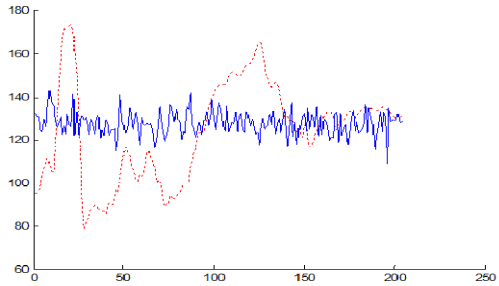

Figure 18(b)

Figure 18(b): Is the Mean Value Analysis of Original Images and Encrypted Image Using HenonMap

CONCLUSIONS

This paper presents a newfangled way of multimedia encoding using a chaotic logistic map. To make the encoding processfurther robust against any attack image was first shuffled to create confusion than encoding in applied. Finally DCT is applied to compress images. To ascertain the good performance of the concocted algorithm histogram analysis and key sensitivity analysis, entropy analysis, mean value analysis, key randomness analysis is done and results are compared with henon map and discussed. Finally, we conclude that proposed method of multimedia encryption expected to be applied in real time encoding and transmission.

REFERENCES

1. N. S. Raghava, Ashish Kumar, “IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE”, International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)ISSN(P): 2249-6831; ISSN(E): 2249-7943Vol. 3, Issue 5, Dec 2013, 11-18.
2. Hazarika, N., Saikia, M., “A Novel Partial Image Encryption using Chaotic Logistic Map’’, Signal Processing and Integrated Networks (SPIN), 2014 International conference on digital signal processing. 10.1109/SPIN.2014.6776953, pp. 231- 236.
3. Qiu Run-he, Cao Yun, Fu Yu-Zhen, “Integrated Confusion-Diffusion Mechanisms for Chaos Based Image Encryption’’ 2011 4th International Congress on Image and Signal Processing. 10.1109/CISP.2011.610030, pp. 629- 632.
4. Hongjun Liu, XingyuanWang,“Triple-image encryption scheme based on one-time key stream generated by chaos and plain images”, Journal of Systems and Software, Volume 86, Issue 3, March 2013, pp. 826-834.
5. Yunpeng Zhang FeiZuo, ZhengjunZhai, CAI Xiaobin, “A New Image Encryption Algorithm Based on Multiple Chaos System”, International Symposium on Electronic Commerce and Security. 10.1109/ISECS.2008.142, pp. 347-350.
6. TiegangGao, QiaoLun GU, Zengqiang Chen, Renhong Cheng, “An Improved Image Encryption Algorithm Based on Hyper-chaos*’’, 2009 Fourth International Conference on Innovative Computing, Information and Control 10.1109/ICICIC.2009.88, pp. 1281-1284.

7. N. K. Pareek,VinodPatidhar and K.K.Sud “Image encryption using chaotic logistic map”, Image and Vision Computing 24(2006) 926-934, received 10 August 2004; received in revised form 11 August2005; accepted 6 February 2006.
8. Weihai Li, NenghaiYu,“A ROBUST CHAOS-BASED IMAGE ENCRYPTION SCHEME”, Multimedia and Expo, 2009.ICME2009.IEEE International Conference. 10.1109/ICME.2009.5202674, pp. 1034-1037.
9. Ashtiyani, M., Electr. Eng. Dept., IHU, Tehran, Birgani, P.M., Hosseini, H.M., “Chaos-Based Medical Image Encryption Using Symmetric Cryptography”, Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008, 10.1109/ICTTA.2008.4530291, pp 1-5.
10. WANG Juan, “Image Encryption Algorithm Based on 2-D Wavelet Transform and Chaos Sequences”, Computational Intelligence and Software Engineering, 2009. CiSE 2009, 10.1109/CISE.2009.5362955, pp. 1-3
11. GuoshengGu, Guoqiang Han, “An Enhanced Chaos Based Image Encryption Algorithm”, Innovative Computing, Information and Control, 2006.ICICIC '06, 10.1109/ICICIC.2006.46, pp.492-495.
12. Hegui Zhu, Cheng Zhao, Xiangde Zhang, “A novel image encryption–compression scheme using hyper-chaos and the Chinese remainder theorem” Signal Processing: Image Communication, Volume 28, Issue 6, July 2013, pp. 670–680
13. Gan Yu, YongjunShen; Guidong Zhang; Yanhua Yang, “A Chaos-based Color Image Encryption Algorithm”, Computational Intelligence and Design (ISCID), 10.1109/ISCID.2013.13, pp. 92-95.